Privacy in transformational government (t-government): an investigation of citizens' privacy preferences and perceptions

Hasbullah, N.A.; Combe, C.

Published in:
Journal of Fundamental and Applied Sciences

Publication date:
2017

Document Version
Publisher's PDF, also known as Version of record

Journal of Fundamental and Applied Sciences

ISSN 1112-9867

Available online at http://www.jfas.info

Research Article

Special Issue

PRIVACY IN TRANSFORMATIONAL GOVERNMENT (T-GOVERNMENT): INVESTIGATION OF CITIZEN'S PRIVACY PREFERENCES AND PERCEPTIONS

N. A. Hasbullah[1,*] and C. Combe[2]

[1]Department of Computer Science, Faculty of Defence Science and Technology, UniversitiPertahananNasional Malaysia, Sungai Besi Camp, 57000 Kuala Lumpur, Malaysia

[2]Department of Business Management, Glasgow Caledonian University, Cowcaddens Road, Glasgow, Scotland, United Kingdom, G4 0BA

Published online: 10 September 2017

ABSTRACT

Transformational government (t-government) was initiated in 2006 in the UK as part of a broader ranging public sector reform agenda. Three main perspectives of t-government feature citizen centricity, shared service culture and professionalism as enablers of integrated citizen-customer feedback for policy development and the reengineering of public services by using Information Society Technologies (IST). These initiatives have seen as an effort of upholding democracy process in giving citizen's their right to address their needs. Protecting citizen's information privacy and security is one of the essential components in the citizen centric model. In addition, the development of a privacy policy for t-government needs to feature citizen opinion and expressed preferences on sensitive information.

Keywords: transformation government (t-government); privacy preference; sensitivity classification.

Author Correspondence, e-mail: asiakin@upnm.edu.my

doi: http://dx.doi.org/10.4314/jfas.v9i3s.39

1. INTRODUCTION

Electronic government (e-government) were always been seen as improving the government service delivery from manually attended to automating the process with the capability to be done in own personal doorsteps [1]. In 2006 the UK government introduced to transformation government (t-government) which defines as citizen-centricity, shared service culture and professionalism after its e-government reached the maturity level. T-government aims for public services to be transformed for benefit of citizens, businesses, tax payers and frontline staff. It is axiomatic of t-government hat shared services will improve the efficiency of service delivery and the government organizational infrastructure which supports open resources in frontline delivery. Increased professionalism is also a key element of t-government and includes all necessary steps to achieve the effective delivery of government services by nurturing capacity and skills in public services [2]. A collaborative environment is then viewed as a key tool for information sharing between government agencies using a single online portal to improve service delivery [3]. The effectiveness of the public sector organizations' activities depend on the collaboration and information sharing between departments and stakeholders [4]. Managing and protecting citizens' information is a challenge that government has to meet to gain public trust. There are three key elements in citizen-centric online public services delivery [5]. These include designing public services to fulfil citizen need, information transparency for ease of access and efficiency in service delivery [6-7]. In addition, there are three important key components to the citizen oriented model to comply under the rubric of citizen centricity-an interface based on citizen life needs; trust-enhancing protection of citizens' information privacy and security; efficiency and accountability through reform of government business processes to reduce cost [6].

The implementation of t-government provides greater involvement of citizen in political and policy making [8]. An adequate security and privacy is a pre-requisite for acceptance by the public as these issues are most frequently cited as barriers to the successful roll-out of electronic government strategies [9-11]. The issues of security and privacy are not limited to the availability and delivery of government services, but also include building citizen trust and confidence in the usage [10, 12]. Previous research done in adoption of Malaysia's

e-government provides evidence that there is concern over privacy issues expressed by citizens [13]. The aim of public service delivery is to fulfil citizen's needs. However, to date citizen participation and involvement has been denied in the design and provision of services [14]. It is argued here that from a citizens' privacy perspective online service provision should be designed based on citizens' opinions and preferences relating to sensitive information as it is an integral element in the design of a privacy policy. The development of an effective privacy policy for t-government needs to take into account citizens' opinions and preferences on sensitive information. With the implementation of t-government, citizens should be able to participate in the provision of policy which will represent the citizen needs. This study investigates Malaysian citizen's privacy preference and priority through sensitivity classification as part of initial investigation for developing privacy framework in t-government.

According to [15], information that unfavourably disturbs one's privacy is characterized as personal data. In addition, the term 'personal' and 'private' are regarded as prima facie synonymous under the UK Data Protection Act (1998) [16]. In [15] survey reveals that the meaning of 'private' data derives connotations of 'control disclosure' and 'sensitive information'. From [16], there is an official difference between 'data' and 'information' but in reality there are no substantial differences [17]. The relevant part of the Act relating to Act sensitive data states:

"In this Act "sensitive personal data" means personal data consisting of information as to-The racial or ethnic origin of the data subject, his political opinions, his is religious beliefs or other beliefs of a similar nature, whether he is a member of a trade union (within the meaning of the M1Trade Union and Labor Relations (Consolidation) Act 1992), his physical or mental health or condition, his sexual life, the commission or alleged commission by him of any offence, or any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings." Sensitive data were originally introduced under the Council of Europe Convention (1981) on Personal Data. Article 6 of the CoE3 Conventions and these international instruments has been a model in some countries enacting data protection laws [18-19]. Article 6 states that:

"Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions."

For comparative purposes it is necessary to set out the relevant legal framework covering data protection in Malaysia. Malaysia is part of the Commonwealth and subject to the unification of laws enshrined in the Federation of Malaya Independence Act 1957 [20]. UK law has been influential in the framing of laws throughout the Commonwealth including that of Malaysia. Evidence of this can be seen in the similarities between the implemented Data Protection Act (1998) in the UK and the Malaysian Personal Data Protection Act 2010 [21]. The latter states that:

"Any personal data consisting of information as to the physical or mental health or condition of a data subject, his political opinions, his religious beliefs or other beliefs of a similar nature, the commission or alleged commission by him of any offence or any other personal data as the Minister may determine by order published in the Gazette;".

Furthermore, Malaysia always refers to the UK in most of its specification and requirements for reference documents. Obvious examples are for the Electronic Record Management Systems-System Specifications and Public Offices Version 3 of National Archives of Malaysia 2011 do indicated that it was adapted from the National Archives (UK), Requirements for Electronic Records Management Systems 3: Reference Document, 2002 [22]. In 2006 the Information Commissioner's Office (ICO) in the UK has done a survey through telephone interview to examine public perceptions of sensitive data. The data are tabulated in Table 1. Significantly this survey was done in the same year as t-government initiated. According to [23] the current prima facie does not reflect sensitivity perception of the data subjects. Therefore, the findings suggested that categories of sensitive data should emerge due to society and technological changes.

Table 1. Sensitivity classification from ICO Survey in United Kingdom [23]

Data Type	Do Not Know	Not Sensitive	A Little Sensitive	Sensitive	Very Sensitive	Extremely Sensitive
			Legally recognized			
Trade union Membership	1.4%	21.6%	13.9%	30.6%	15.1%	17.4%
Religious/philosophical belief	0.9%	21.4%	12.1%	28.2%	13.3%	24.0%
Political Opinion	0.9%	15.9%	13.1%	28.1%	17.4%	24.5%
Race or Ethnic Origin	1.3%	19.5%	11.2%	1.3%	16.6%	24.6%
Criminal Records	1.1%	11.2%	7.2%	22.9%	17.5%	40.1%
Sexual Live Information	1.6%	6.8%	6.7%	18.0%	17.1%	49.8%
Physical and mental health	0.9%	3.8%	5.1%	18.2%	20.6%	51.3%
			Not Legally recognized			
Employment History	1.1%	15.9%	12.1%	30.2%	19.3%	21.3%
Education Qualification	1.4%	15.9%	11.7%	29.5%	19.5%	22.0%
Political Membership	1.5%	17.4%	13.4%	30.1%	15.5%	22.0%
Click stream data	2.5%	15.9%	11.4%	27.5%	18.2%	24.4%
Personal Contact Detail	0.4%	7.0%	7.1%	17.8%	21.4%	46.2%
Genetic Information	1.6%	8.7%	6.3%	20.8%	19.2%	43.3%
Biometric Information	2.2%	10.4%	6.8%	17.5%	17.6%	45.4%
Financial Data	0.6%	1.9%	2.5%	7.1%	17.4%	70.5%

2. METHODOLOGY

A survey was conducted to gauge the citizens' privacy preferences. The survey was done to respondents from Kuala Lumpur and the state of Selangor, Malaysia.

2.1. Research Framework and Instrument

The main constructs of sensitive data were used to investigate the citizens' privacy preferences. Sensitive data was based on [24] who cited that serious attempt to determine

privacy sensitivity level to each personal data element during system design phase and [25] to defines the category of sensitive information in order to restrict access to intimate, sensitive or confidential information.

2.2. Data Collection

To investigate Malaysia sensitivity preference and priority a survey has been done in Kuala Lumpur and in Selangor State of Malaysia. Convenience sampling of 227 respondents from the urban area and 123 people from the rural area have been chosen to answer a closed questionnaire. To ensure a fair representation of the diverse Malaysian demographic, 64.6% of the respondents were Malays, 19.4% Chinese, 11.7% Indians and 4.3% other ethnic groups. The current Malaysian population of ethnic groups is 67.4% Bumiputra (63.1% Malays and 4.3% other predominant ethnic group), 24.6% Chinese, 7.3% Indians and 0.7% others [26]. The gender balance comprised 45.1% males and 54.9% females. In addition, the cumulative of percentage of professionals involved in the survey was 48.3%. In the questionnaire, the definitions of personal and sensitive data are clarified to ensure respondents understand their meaning. Through the questionnaire, respondents were asked to classify types of personal and sensitive data by ticking between sensitive and personal data; and not sure for data that respondents donot know or want it to fall neither personal nor sensitive. Research done by [27] revealed that scales consisting of three points are sufficient [28-29].

3. RESULTS AND DISCUSSION

Data was processed using SPSS 16.0 for descriptive statistic and the citizens' preferences are tabulated according to priority in Table 2.

Table 2. Malaysia personal and sensitive data

	Sensitive	Personal	Not Sure
Biometric Information	62.9%	28.3%	8.9%
Financial Detail	60.0%	31.7%	8.3%
Sexual Life Information	52.6%	34.3%	13.1%
Genetic Information	51.7%	38.9%	9.4%
Political pinion	50.6%	33.4%	16.0%
Physical or Mental Health	50.0%	39.4%	10.6%
Offense or Criminal records	48.3%	32.3%	19.4%
Identity Card Number	47.1%	44.9%	8.0%
Telephone Number	42.0%	49.1%	8.9%
Map of your house	40.9%	48.0%	11.1%
Religion or Belief	35.7%	50.3%	14.0%
Home Address	35.7%	54.9%	9.4%
Racial or Ethnic Origin	33.7%	54.3%	12.0%
Employment History	28.3%	60.6%	11.1%
Email Address	27.4%	57.4%	15.1%
Workplace	24.0%	65.4%	10.6%
Academic Qualification	19.7%	70.6%	9.7%

From the survey, 62.9% classified “biometric information” as sensitive and 28.3% classified it as personal in which, if calculated in total, is the highest level of sensitivity. Since 1st June 2011, Malaysia had implemented a fingerprint biometric system for immigration purposes at all Malaysian borders [30]. There are government agencies and companies that also implement a fingerprint system for authentication for entry to buildings and at the same time to monitor employees clocking in and out times. A study by [31] indicated that the highest percentage of 60.1% of Malaysians for either agreed or strongly agreed with the statement that “biometric devices are an invasion of privacy” followed by Australia with 27.8% and the United States of America (USA) with 21.4%. In addition, every citizen of Malaysia is issued with a unique identification card (MyKad). This card is embedded with chips that carry

information including photos and fingerprints as a biometric authentication. Malaysians when they deal with government agencies, banks or hospitals they have to produce their identity card and get their thumb scanned whenever authorization is needed [32]. From the survey, 47.1% of respondents classified the "identity card" as sensitive and only 44.9% classified it as personal.

More than half of the respondents classified "Financial detail" as sensitive compare to others. From this opinion the highest percentage of sensitive information is data that have a connection or risk to citizen financial outcome. "Financial detail" registers second in the list of sensitive information after "biometric information" with 60.0% for sensitive and 31.7% classified it as personal. Here, "financial detail" refers to bank account data, cash transactions, any bank loans, credit and debit card transactions and anything involving an individual's financial matters. Previous research undertaken indicated that 62% of respondents answer the reasons for choosing "financial data" as privacy priority as it "may lead to financial loss" [33]. This survey evidenced that 52.6% classified "sexual life information" as sensitive and 34.3% classified it as personal. Malaysia has an enactment under Islamic law (sharia law) for prosecuting sex offenses in which these laws are made specific to the Muslims [34]. This provides the primary reason for the fact that sexual activity was not classified under sensitive information in the Malaysia Data Protection Act as it could cause a conflict in judgement.

Hence, "Genetic information" should be classified as sensitive information as it might potentially cause prejudice and unfairness as a result of inappropriate disclosure [23]. "Genetic information" is important as, for example, it can inform the judgement of health insurers when assessing risk. For example, insurers do not offer coverage to those who have deoxyribonucleic acid (DNA) that raises the risk of contracting breast cancer [35]. So, although having a DNA structure that places an individual in a higher risk category, it does not follow that the individual will contract the condition [36]. In this survey, 51.7% classified "genetic information" as sensitive and 38.9% classified it as personal. In Malaysia" it is normal procedure to forfeit genetic information for entering university [37], applying for scholarship or jobs. Malaysians are required to declare their family medical history and agree to the terms and conditions of employment that includes being rejected if false information is

given.

In addition, 50.6% classified "Political opinion" as sensitive and 33.4% classified it as personal. Malaysia has been ruled by the same component of the dominant political party which is BarisanNasional (BN) since its independence from British colonial in 1967 [38]. In 2008, BN lost the two third of a majority in parliament as the opposition made greater use of the internet which have been proven its ability to be accessed by citizens [39]. The internet facilitates the information to be obtained through social networks and blogs, whereby political opinions and agenda are made public by opposition and citizens without any barriers and secrecy [40]. "Political opinion" will be sensitive during polling day or a general election when personal votes are secret.

For "Physical and mental health" only 50.0% of respondents classified it as sensitive and 39.4% as personal. "Physical and mental health" is considered sensitive by certain people with conditions that they would prefer to keep private. Much depends on the type and nature of the condition. For example, HIV/AIDS carries not just a physical consequence but also a social stigma [41]. In June 2009 the Malaysian conference of the Fatwa Committee of the National Council of Islamic Religious Affairs made mandatory an HIV test to prospective Muslim brides and grooms to prevent greater harm to the spouse and future generations [42-43]. It is a normal procedure in Malaysia to attend a medical examination and have the chest x-rayed to enable one to be accepted to a public higher education institution [37], public or private universities, government and large private companies during recruitments. These and other examples account for the reason why Malaysians are less sensitive about health.

"Offense or Criminal records" were classified as sensitive for 48.3% of respondents, while 32.3% classified it as personal. In Malaysia, for ex-convicts who are citizens of Malaysia, the government issues a new identity card containing a brown stripe to denote that a prison sentence has been served by the holder [44]. Here, an employer or future employer can check the criminal record of that person and the type of prosecutions that they faced [49]. In this survey, personal contact detail has been divided into "home address", "workplace", "telephone number" and "email address" with a total sensitive of 35.7%, 24%, 42% and 27.4% respectively. It is common for citizens receive sales and marketing calls from insurance agents,

credit card sales people and mutual financial consultants among others to promote their products and services. Most of these companies are subsidiaries of banks that enable them to obtain customer information from the holding's customer list. Nevertheless, personal contact details are classified as less sensitive as this information is essential in most of the form or to be provided when perform any registering to government agency, banks, privilege cards and even a survey.

"Religion or belief" and "race or ethnic origin" was classified as sensitive by 35.7% and 33.7% for sensitive respectively. There are three major ethnics in Malaysia which are Malays, Chinese and Indians. Malay people are considered the indigenous population of Malaysia within the multi-ethnic society that was created during British colonial rule [45-46]. This coincided with the immigration of Chinese people who sought to exploit local resources and ventures by planting cash crops such as sugar cane, pepper, spices and coffee for commercial purposes. The immigration of Indians for labour purposes [47] was another feature of demographic change during this era. In the Malaysian Data Protection Act 2010, "ethnic and racial origin" was not classified as sensitive information yet it was vice versa for "religion or belief". It is a normal interpretation in Malaysia that Malays are Muslim, Chinese are Buddhist and Indians are Hindus [48]. There are cases of converts to Islam and Christians by Chinese and Indians, but to have converters from Islam will be an isolated case. Table 3 compared all the sensitive information selected by more than 50% of respondents as sensitive with the Malaysian Personal Data Protection Act (2010).

Table 3. Comparison between sensitive information from the citizen and the Personal Data Protection Act (2010)

Sensitive Information from Citizens	**Sensitive Information from Personal Data Protection Act 2010 (Malaysia)**
Physical or Mental Health, Political Opinion, Biometric Information, Financial Detail, Sexual Life Information, Genetic Information	Physical or Mental Health, Political Opinions, Religious beliefs or other beliefs of a similar nature. The commission or alleged commission by him of any offense or any other personal data as the Minister may determine

From the comparison, only “physical or mental health” and “political opinion” are listed as sensitive information in the Personal Data Protection Act 2010 (Malaysia) whereas others differ from the citizen's opinion.

4. CONCLUSION

It is evidenced that the current prima facie does not reflect the sensitivity preferences and perception of the citizens which supported by the findings of [23]. From the findings, she suggested the categories of sensitive data should emerge due to society and technological changes. Through our findings, we suggested that categories of sensitive data for system development should come from the citizens as a user and potential user of the e-government system. With the t-government around the corner, provisioning of policy to represent citizens’ requirements and needs should take into account citizen participation in protecting their privacy. This survey evidenced that data, which are related to one’s financial outcomes was selected as the highest sensitive data from other types of data. Moreover, most of the highest priorities of sensitive data are data that was derived from new technology and not legally recognized in the Data Protection Act. With the implementation of t-government, most of the data are stored and made available in the network which increase the risk or possibilities to be compromised. Through the addition of these data types shows that the classification of sensitive information might have possibilities of changes over the time. Therefore, the results from this study should be able to assist and will be a basis in the development of a privacy framework in t-government in which will be able to design an effective privacy policy.

5. ACKNOWLEDGEMENTS

List here those individuals who provided help during the research (e.g., providing language help, writing assistance or proof reading the article, etc.).

6. REFERENCES

[1] Waller P., Weerakkody V. Digital government: overcoming the systemic failure of transformation. London: Brunel University Press, 2016

[2] Irani Z, Sahraoui S, Ozkan S, Ghoneim A, Elliman T. T-government for benefit realisation. In European and Mediterranean Conference on Information Systems, 2007, pp. 1-11

[3] Mohammed M A, Maroof E Y, Thamer A, Huda I. What are the electronic information sharing factors that influence the participation behavior in higher education sector? Procedia Computer Science, 2015, 72:49-58

[4] Combe C. Observation on the UK transformational government strategy relative to citizen data sharing and privacy. Transforming Government: People, Process and Policy, 2009, 3(4):394-405

[5] Sigwejo A, Pather S. A citizen-centric framework for assessing e-government effectiveness. Electronic Journal of Information Systems in Developing Countries, 2016, 74(8):1-27

[6] Cai H, Wang K. Service oriented design method and practice for constructing citizen-centric public services. In IEEE International Conference on e-Business Engineering, 2006, pp. 536-540

[7] Venkatesh V, Thong J Y, Chan F K, Hu P J. Managing citizens' uncertainty in e-government services: The mediating and moderating roles of transparency and trust. Information Systems Research, 2016, 27(1):87-111

[8] Sharif A M. Transformational government: What is the shape of things to come? (Invited Viewpoint). Transforming Government: People, Process and Policy, 2008, 2(1):71-75

[9] Jin-Fu W. E-government security management: Key factors and countermeasure. In 5th IEEE International Conference on Information Assurance and Security, Xi'an, 2009, pp. 483-486

[10] Ebrahim Z, Irani Z. E-government adoption: Architecture and barriers. Business Process Management, 2005, 11(5):589-611

[11] Layne K, Lee J. Developing fully functional e-government a four stage model. Government Information Quarterly, 2001, 18(2):122-136

[12] Mohamed M Z, Xavier J A. Transforming public service delivery in Malaysia: The case of implementation of e-government in local governments. Journal of Contemporary Management Research, 2016, 10(1):39-57

[13] Jasber K, Noor D N R. Malaysian electronic government adoption barriers. Public Sector ICT Management Review, 2008, 2(1):38-43

[14] Taher Y, Heuvel W J, Koussouris S, Georgousopoulos C. Empowering citizens in public service design and delivery: A reference model and methodology. InEuropean Conference on a Service-Based Internet, 2010, pp. 129-13

[15] McCullagh K. Protecting 'privacy' through control of 'personal' data processing: A flawed approach. International Review of Law, Computer and Technology, 2009, 23(1-2):13-24

[16] legislation.gov.uk. Data Protection Act 1998. London: Parliament of the United Kingdom, 1998

[17] Korff D. Comparative summary of national laws. Brussels: EC Study on Implementation of Data Protection Directive, 2002

[18] Wong R. Data protection online: Alternative approaches to sensitive data? Journal of International Commercial Law and Technology, 2007, 2(1):9-16

[19] Bygrave L. A. Data protection law: Approaching its rationale, logic and limits.New York: Aspen Publishers, 2003

[20] Wortley B A. Great Britain and the movement for the unification of private law since 1948. Tulane Law Review, 1958, 32(4):541

[21] Laws of Malaysia. Act 709: Personal Data Protection Act 2010.Kuala Lumpur: PercetakanNasional Malaysia Berhad, 2010

[22] Arkib Negara Malaysia (ANM). Guest: Elektronik. Kuala Lumpur: ANM, 2015

[23] McCullagh K. Data sensitivity: Proposals for resolving the conundrum. Journal of International Commercial Law and Technology, 2007, 2(4):32-39

[24] Skinner G, Chang E. PP-SDLC: The privacy protecting system development life cycle. In IPSI, 2005, pp. 1-17

[25] Nissenbaum H. Privacy a contextual integrity. Washington Law Review, 2004, 79:101-139

[26] Department of Statistics Malaysia (DOSM). Preliminary count report population and housing census Malaysia.Putrajaya: DOSM, 2010

[27] Friedman H H, Amoo T. Rating the rating scales. Journal of Marketing Management,

1999, 9(3):114-123

[28] Jacoby J, Matell M S. Three-point Likert scale are good enough. Journal of Marketing Research, 1971, 8(4):495-500

[29] Lehmann D R, Hulbert J. Are three-point scales always good enough? Journal of Marketing Research, 1972, 9(4):444-446

[30] FreeMalaysiaToday.com. Malaysia starts fingerprinting visitor. Selangor: MToday News Sdn. Bhd., 2011

[31] Weerakkody N. A Comparative analysis of opinions of Americans, Australians and Malaysian on the use of biometric devices in workplaces for security and monitoring of worker productivity. International Journal of Management, 2005, 5(6):43-52

[32] Masrom M. Chapter 13: E-government, e-surveillance, and ethical issues from Malaysian perspective. In R. A. Cropf (Ed.), Ethical issues and citizen rights in the era of digital government surveillance. Pennsylvania: IGI Global, 2016, pp. 249-263

[33] Hasbullah N A, Aziz AA, Ismail S, Hamid N N. Initial investigation on privacy preferences: A preliminary study on user priority, concern, perception and expectation. International Journal on Advanced Science, Engineering and Information Technology, 2011, 1(2):217-220

[34] Ismail S Z. The legal perspective of *khalwat* (close proximity) as a *shariah* criminal offence in Malaysia. Pertanika Journal of Social Sciences and Humanities, 2016, 24(3):923-935

[35] Jingquan L. Genetic information privacy in the age of data-driven medicine. In IEEE International Congress on Big Data, 2016, pp. 299-306

[36] National Institute of Health (NIH). Genetic Information Nondiscrimination Act 2008. Maryland: NIH, 2012

[37] Ministry of Higher Education (MoHE). Medical report. Putrajaya: MoHE, 2012

[38] BarisanNasional (BN). BarisanNasional-Rakyat didahulukan. Kuala Lumpur: BN, 2010

[39] Abdul R M. 2004 and 2008 general elections in Malaysia: Towards a multicultural, bi-party political system? Asian Journal of Political Science, 2009, 17(2):173-194

[40] Salman A, Mustaffa N, Salleh M A M, Ali M N S. Social media and agenda setting:

Implications on political agenda. JurnalKomunikasi-Malaysian Journal of Communication, 2016, 32(1):607-623

[41] Syed I A, Sulaiman S, Azhar S, Hassali M A, Thiruchelvum K, Lee C K. A qualitative insight of HIV/AIDS patients' perspective on disease and disclosure. Health Expectations, 2015, 18(6):2841-2852

[42] JabatanKemajuan Islam Malaysia (JAKIM). KerajaanmewajibkanperlaksanaanujiansaringanHIV kepadabakalpengantin. Putrajaya: JAKIM, 2009

[43] Saidon R, Kamaruddin Z, Ariffin M, Ibrahim N, Sahari N H. Examining the policy of mandatory premarital HIV screening Pertanika Journal of Social Sciences and Humanities, 2015, 23(S):129-140

[44] Parliament of Malaysia (PoM). Dewan Rakyat. Kuala Lumpur: PoM, 2011

[45] Chin L C. Immigration control during the Malayan emergency: Borders, belonging and citizenship. Journal of the Malaysian Branch of the Royal Asiatic Society, 2016, 89(1):35-39

[46] Koh S Y. How and why race matters: Malaysian-Chinese transnational migrants interpreting and practisingBumiputera-differentiated citizenship. Journal of Ethnic and Migration Studies, 2015, 41(3):531-550

[47] C. Hirschman. Ethnic and social stratification in Peninsular Malaysia. Washington DC: American Sociological Association, 1975

[48] Chan A, Islam M S. State, religion, and environmentalism: fostering social cohesion and environmental protection in Singapore. Environmental Sociology, 2015, 1(3):177-189

[49] Nazni N, Zaherawati Z, MohdZoolHilmie M S, Kamarudin N, Zaliha H H. Bankruptcy among young executives in Malaysia. In International Conferences on Economics Marketing and Management, 2012, pp. 132-136

How to cite this article:
Hasbullah N A, Combe C. Privacy in transformational government (t-government): investigation of citizen's privacy preferences and perceptions. J. Fundam. Appl. Sci., 2017, *9(3S), 503-517*